IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA

IN THE MATTER OF THE SEARCH OF Contents of a file submitted in connection with CyberTipline Report # 197635988, currently in custody of Homeland Security Investigations, and more fully described in Attachment A.	**Case No. 2:25-mj-00007**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEIZURE AND SEARCH WARRANT

I, Andrew C. Hayden, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent ("SA") with Homeland Security Investigations ("HSI"), United States Department of Homeland Security ("DHS"). As such, I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510 (7), and am empowered by law to conduct investigations and to make arrests for offenses enumerated in Title 18, United States Code Section 2252.

2. I have been a SA with HSI since 2017. I am a graduate of the Criminal Investigations Training Program ("CITP") and the Homeland Security Investigations Special Agent Training Program ("HSISAT") at the Federal Law Enforcement Training Center at Glynco, Georgia. Prior to HSI, I was the Chief Criminal Investigator for the Missouri Bureau of Narcotics and Dangerous Drugs and a Criminal Investigator for the Missouri Department of Corrections. I have a master's degree in Homeland Security with a primary emphasis in Criminal Justice. My

duties as a SA include, but are not limited to, the investigation and enforcement of Titles 8, 18, 19, 21 and 31 of the United States Code (U.S.C.)

3. As a part of my daily duties as an HSI SA I investigate criminal violations relating to child pornography and the sexual exploitation of minors, to include the receipt or distribution of child pornography as defined by 18 U.S.C. § 2252A. In my career, I have had the opportunity to participate in and conduct investigations related to cybercrime and child exploitation on numerous occasions.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all knowledge of our investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

5. I have obtained the information contained in this affidavit from my personal participation in the investigation and from reviewing information obtained through legal process, as well as from information obtained through law enforcement and commercial databases.

6. I have not included each and every fact known to me concerning the underlying investigation, as the sole purpose of this affidavit is to establish the required foundation for the requested search warrant. I have set forth only the facts that I believe are essential to establish this required foundation. Facts not set forth herein are not being relied upon in reaching my conclusion that a warrant should be issued. I do not request that this Court rely upon any facts not set forth herein in reviewing this affidavit and accompanying application.

7. I make this affidavit in support of an application for a search warrant for files (**TARGET FILES**) submitted by an Electronic Service Providers ("ESP") to the National Center for Missing and Exploited Children ("NCMEC") in connection with the following Cyber Tipline Report, currently located in the Southern District of West Virginia.

(hereafter, the **TARGET FILES**):

CyberTipline Report Number: 197635988

Electronic Service Provider: Google

Date Received by NCMEC (in Coordinated Universal Time, UTC): August 12, 2024 at 23:34:12 Coordinated Universal Time (UTC)

8. I am investigating the use of Google accounts, referenced in the above-described CyberTipline Report, to possess, receive and/or distribute child sexual abuse material ("CSAM"). As will be shown below, there is probable cause to believe this individual violated 18 U.S.C. §§ 2252(a)(2) and (b)(1), the receipt and/or distribution of child pornography and 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2), possession of child pornography ("**the TARGET OFFENSES**"), and that contraband, evidence, fruits and instrumentalities of violations of the **TARGET OFFENSES** will be found with the **TARGET FILES**.

9. The facts set forth in this affidavit are based on my personal observations, my training and experience, my review of records, as well as information provided by other law enforcement officials and Internet Crimes Against Children (ICAC) Task Force. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge about this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and

in part only. Furthermore, the opinions and conclusions set forth below are based on my training and experience as a Special Agent, my discussions with other experienced law enforcement officers, and my participation in this investigation. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of the **TARGET OFFENSES** are present within the **TARGET FILES**.

DEFINITIONS AND TECHNICAL TERMS

10. The following definitions and technical terms apply to this Affidavit and Attachment B.

a. Computer" means "an electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, and mobile phones, tablets and other portable devices. *See* 18 U.S.C. § 1030(e)(1).

b. "Computer passwords and data security devices" means information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates

"test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

c. "Internet Protocol address" or "IP address" means a unique number used by a computer or other digital device to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.

d. "Internet Service Providers" ("ISPs") means commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

e. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. "Minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

g. "Records," "documents," and "materials," each mean all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

h. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. §2256(2).

i. A "storage medium" means any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

j. "Visual depiction" means undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. §2256(5).

k. "Chat" means any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

l. "Mobile applications" means small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game).

BACKGROUND ON THE CYBERTIPLINE AND NCMEC

11. NCMEC is a private, non-profit organization established in 1984 by the United States Congress. Primarily funded by the Department of Justice, NCMEC acts as an information

clearinghouse and resource for parents, children, law enforcement agencies, schools, and communities to assist in locating missing children and to raise awareness about ways to prevent child abduction, child sexual abuse and depictions of minors engaged in sexually explicit conduct.

12. The NCMEC CyberTipline offers a means of reporting incidents of child sexual exploitation, including the possession, manufacture, and/or distribution of depictions of minors engaged in sexually explicit conduct; online enticement; child prostitution; child sex tourism; extra familial child sexual molestation; unsolicited obscene material sent to a child; and misleading domain names, words, or digital images.

13. Federal law requires NCMEC to operate the CyberTipline and requires Electronic Service Providers ("ESPs") to report apparent instances of child pornography offenses. Providers also have the discretion to submit reports concerning planned or imminent child pornography offenses. Companies that suspect child pornography has been stored or transmitted on their systems report that information to NCMEC in a CyberTipline Report (or "CyberTip"). The ESP submits the report, which generally contains account and log-in information, and uploads content to NCMEC via a secure connection. Aside from required information such as incident type, date, and time, reporters can also fill in voluntary reporting fields such as user or account information, IP addresses, or information regarding the uploaded content itself, as well as other information it may have collected in connection with the suspected criminal activity. The ESP may or may not independently view the content of the file(s) it uploads. Using publicly available search tools, NCMEC then attempts to locate where the activity occurred based on the information the ESP submits, such as IP addresses. NCMEC then packages the information from the ESP along with any additional information it has, such as previous related CyberTips, and sends it to law enforcement in the jurisdiction where the activity is believed to have occurred.

HASH VALUES AND HASH MATCHING

14. Based on my training and experience, my conversations with other law enforcement officers, and information I have learned from ESPs, I know that when an ESP receives a complaint or other notice of suspected depictions of minors engaged in sexually explicit conduct, they may employ a "graphic review analyst" or an equivalent employee to open and look at the image or video file to form an opinion as to whether what is depicted likely meets the federal criminal definition of depictions of minors engaged in sexually explicit conduct found in 18 USC § 2256. If the employee concludes that the file contains what appears to be depictions of minors engaged in sexually explicit conduct, a hash value of the file can be generated by operation of a mathematical algorithm and assigned to the image.

15. A hash value is an alphanumeric sequence that is unique to a specific digital file. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, results in a different hash value. Consequently, an unknown image can be determined to be identical to an original file if it has the same hash value as the original. The hash value is, in essence, the unique fingerprint of that file, and when a match of the "fingerprint" occurs, the file also matches. I know from my training and experience that the chances of two files with different content having the same hash value are infinitesimal.

16. When a NCMEC employee or law enforcement agent determines that an image depicts minors engaged in sexually explicit conduct, a unique hash value will similarly be assigned to that image.

17. ESPs typically maintain a database of hash values of files that they have determined to meet the federal definition of depictions of minors engaged in sexually explicit conduct found in 18 USC § 2256. The ESPs typically do not maintain the actual suspect files themselves; once a file is determined to contain suspected depictions of minors engaged in

sexually explicit conduct, the file is deleted from their system. NCMEC also maintains a database of the hash values.

18. The ESPs can then use Image Detection and Filtering Process ("IDFP"), Photo DNA (pDNA), or a similar technology which compares the hash values of files embedded in or attached to transmitted files against their database containing what is essentially a catalog of hash values of files that have previously been identified as containing suspected depictions of minors engaged in sexually explicit conduct.

19. When the ESP detects a file passing through its network that has the same hash value as an image or video file that was previously determined to depict minors engaged in sexually explicit conduct, the ESP reports that fact to NCMEC via the latter's CyberTipline. By statute, as described above, an ESP has a duty to report to NCMEC any apparent depictions of minors engaged in sexually explicit conduct it discovers "as soon as reasonably possible." 18 U.S.C. § 2258A(a)(1).

20. Because images previously determined to contain depictions of child sexual abuse material (CSAM) carry a known hash value, an ESP may flag and report images in a user account to NCMEC without also contemporaneously reviewing the images. Based on my training and experience and conversations with ESPs, in this situation, the ESP's decision to report a file to NCMEC is made because the hash value of the reported image is identical to the hash value of the previously reviewed image depicting minors engaged in sexually explicit conduct.

INDUSTRY CATEGORIZATION OF CSAM FILES

21. Based on my training and experience, I know that beginning in 2014, some of the ESPs including Google, Facebook, Dropbox and Snapchat developed industry categories to describe some of the content depicted in the images reviewed by the ESPs. The ESPs will

include this category, when available, when submitting the image file to NCMEC. The categories are described below.

Category 1 (A = pre-pubescent child) and (B = pubescent child): "Sex Act": Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.

Category 2 (A = pre-pubescent child) and (B = pubescent child: "Lascivious Exhibition": Any image depicting nudity and one on more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

PROBABLE CAUSE

22. On or about November 19, 2024, I became aware of a CyberTip which had been reported to NCMEC from Google. As described above, this warrant seeks authorization to search the **TARGET FILES** submitted to NCMEC with the CyberTip # 197635988.

23. CyberTip # 197635988 was submitted to NCMEC on or about August 12, 2024, by Google. The CyberTip report indicated Google was submitting two files to NCMEC. The first file, which was a file in mp4 format suspected to contain CSAM had been uploaded to a Google account on or about April 30, 2024, at 11:43:02 UTC. The second file, which was a file in jpg format suspected to contain CSAM had been uploaded to a Google account on or about August 11, 2024, at 19:30:29 UTC. The report indicated that Google employees had not contemporaneously reviewed the files of suspected CSAM before submitting the CyberTip.

Based on my training and experience, and my review of the CyberTip report, I understand that Google identified the file as suspected CSAM based on the video file's hash value, which matched the hash value of a previously identified image depicting a minor engaged in sexually explicit conduct. Google further categorized the mp4 file as B1, indicating that the video file depicted a pubescent minor engaged in a sex act and the jpg file as B2, indicating a pubescent minor engaged in lascivious exhibition. The name of the Google account was Arnold JONES and the IP address used to upload the mp4 file was 75.109.235.240 and the IP address used to upload the jpg file was 207.213.211.11. IP address 75.109.235.240 showed to be located in Charleston, West Virginia. The ESP provided additional information that contained the suspect telephone numbers of +16813417058 and +16812050851 that were associated with the Google account. The suspect telephone number +16813417058 showed to be located in Clendinen, West Virginia and the suspect telephone number +16812050851 showed to be located with a Post Office box in Hiawassee, Georgia. Public information showed the area code (681) to be associated with West Virginia. The ESP also provided information that contained the suspect email address jonesarnold607@gmail.com associated with the Google account.

24. I submit that the element of "in or affecting interstate or foreign commerce" is satisfied for a violation of 18 U.S.C. § 2252A and 18 U.S.C. § 2252, for the limited purpose of securing a search warrant, through use of ESP servers and use of the Internet in connection with the offense.

JURISDICTION

26. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

CONCLUSION

27. Based on the foregoing facts, my experience and training, and in consultation with other law enforcement agents experienced in child exploitation investigations, I believe there is probable cause that contraband, evidence, fruits and instrumentalities of violations of the Target Offense will be found within the **TARGET FILES.**

Andrew C. Hayden
Special Agent
Department of Homeland Security
Homeland Security Investigations

Sworn to by the Affiant telephonically in accordance with the procedures of Rule 4.1 this 4th day of Feb, 2025.

DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF WEST VIRGINIA